REMARKS/ARGUMENTS

The applicants acknowledge, with thanks, the Office Action dated April 10, 2009. Examiner's consideration of Applicant's arguments of January 30, 2009, is noted with appreciation. Claims 1, 17, 24, and 27 have been amended above. No claims were canceled and no new claims have been presented. Accordingly, claims 1-2, 5-10, 15-21, 24, and 26-27 are currently pending.

Entry of this amendment is requested pursuant to MPEP 714.12 and 714.13 (37 CFR 1.116) because the amendment adopts suggestions of the examiner for complying with objections and places the application in better form for appeal. Reconsideration of the application as amended and in view of the arguments and comments presented below is respectfully requested.

It is respectfully submitted that the reconsideration of the amended claims will require no further search.

The Non-Art Matters

Claims 1 and 24 were objected to in the Office Action of April 10, 2009 for informalities pointed out by the Examiner. In particular, with regard to independent claim 1, the Examiner took the position that the claim refers to "the subsequent secure tunnel" in the "authenticating" step before any such secure tunnel has been set forth in the claim. In addition, with regard to independent claim 24, the Examiner noted that the claim refers to "the subsequent new tunnel" in the final element thereof before, according to the Examiner, any such subsequent new tunnel has been set forth in the claim.

Claims 1 and 24 have been amended to correct the informalities objected to by the Examiner. Other changes were made as well to help clarify the claim language. It is respectfully submitted that the amendments tendered to the claims introduce no new matter and no further search will be necessary.

In addition, applicants have tendered selected amendments to claims 17 and 27 in a manner corresponding to the changes made in claims 1 and 24 identified by the Examiner. It is respectfully submitted that the amendments tendered to these claims also introduce no new matter and no further search will be necessary.

The Art Matters

Although this amendment is being tendered to address claim objections made by the examiner, applicant would respectfully request the examiner consider the following arguments regarding the prior art rejections. Claims 1-2, 5-6, 9-10, 15-21, 24, and 26-27 were rejected in the Office Action of April 10, 2009 under 35 U.S.C. §103(a) as being unpatentable over Dogan (US Patent Application Publication 2004/0268126) in view of Kuehr-McLaren, (US Patent 6,978,298) and Funk (Paul Funk, Simon Blake Wilson, "draft-ietf-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)"; Internet draft PPPEXT Working Group; 30 Nov. 2002, pp. 1-40). Claims 5-10 and 20 were rejected under 35 U.S.C. §103(a) as being unpatentable over Dogan in view of Kuehr-McLaren and Funk, and further in view of Downnard (Downard, Ian, "Public-Key Cryptography extensions into Kerberos", IEEE December 2002/January 2003, p.30-34).

Independent claim 1, as currently amended, recites a method or system for authenticating communication between a first and second party. A first secure tunnel is established between a peer and a server using asymmetric encryption in response to determining that a shared secret does not exist between the peer and the server. The shared secret is received via the first secure tunnel between the peer and the server and the first secure tunnel is then torn down. A subsequent new secure tunnel is established between the peer and the server using symmetric encryption and the shared secret after tearing down the first secure tunnel and after the peer has received the shared secret. A tunnel key is mutually derived for the subsequent new secure tunnel using symmetric cryptography based on the shared secret in response to establishing the subsequent new secure tunnel. A relationship between the peer and the server is then authenticated within the subsequent secure tunnel. The subsequent new secure tunnel is then cryptographically bound with conversations inside the subsequent new secure tunnel (which is recited in claim 25 as derive keying material that binds the subsequent new tunnel with all conversations inside the subsequent new tunnel). No new matter has been added as the amendments are supported by the original specification (see Figure 6, block 685 and ¶150). Independent claims 17 and 24 recite a system of claim 1.

By contrast, Dogan teaches shared secret generation for symmetric cryptography. A master secret is established between a first communications device and a second communications device. Then a connection is opened between the first communications device and the second

communications device. A connection secret is generated from the master secret and used as a symmetric key during the life of the connection. However, Dogan does not teach or suggest receiving a shared secret via a first secure tunnel established between a peer and a server using asymmetric encryption. Symetric cryptography is based on the use of pre-shared secret. The parties obtain the secret through some protected external means. Asymmetric cryptography, on the other hand, is a zero knowledge approach and provides a higher level of security since a pre-shared secret is not relied on. Dogan teaches establishing a master secret in a fashion similar to exchanging a shared secret (see ¶23). A shared secret is exchanged using symmetric key cryptography (see ¶17). Further, Dogan teaches establishing the master secret during registration in one example (see ¶23). Thus, the master secret taught by Dogan is pre-shared. In contrast, claim 1 recites establishing a shared secret using asymmetric cryptography rather then using a pre-shared secret. This enables claim 1 to achieve a higher level of security.

Additionally, Dogan does not teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the tunnel as recited in claim 1. Cryptographic binding of the tunnel with the conversation inside the tunnel helps prevent man-in-the-middle attacks which enable an adversary to take control of information between a peer and a server. Dogan does not address the prevention of such attacks. Thus, Dogan does not teach or suggest every element of claim 1.

The aforementioned deficiencies in Dogan are not remedied by any teachings of Kuehr-McLaren, Funk, or Downnard. Kuehr-McLaren teaches a method and apparatus for managing session information in a data processing system. A request for a secure connection is received. The secure connection is established, wherein information used to facilitate the secure connection is generated. The information is stored for a selected period of time, wherein the selected period of time is selected to optimize server resources. However, Kuehr-McLaren does not teach or suggest receiving a shared secret via a first secure tunnel established between a peer and a server using asymmetric encryption nor does Kuehr-McLaren teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the tunnel. Kuehr-McLaren is relied on by the Office Action to teach determining whether a shared secret exists between a peer and a server.

Funk teaches using asymmetric encryption for establishing tunnels and the authenticating within the tunnel. However, Funk does not teach or suggest establishing a first secure tunnel

using asymmetric encryption to receive a shared secret for use in subsequent authentications nor does Funk teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the tunnel.

Downnard teaches public key cryptography extensions into Kerberos. However, Downnard does not teach or suggest establishing a first secure tunnel using asymmetric encryption to receive a shared secret for use in subsequent authentications nor does Funk teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the tunnel. Downnard is relied on by the Office Action to teach the shared secret being a protected access credential.

Thus, neither Dogan, Kuehr-McLaren, Funk, nor Downnard, alone or in combination, teach or suggest each and every element of independent claims 1, 17 and 24. Therefore, for the reasons set forth, withdrawal of these rejections is respectfully requested.

Claims 2, 5-10, 15-16, and 27 depend directly from claim 1 and therefore contain each and every element of claim 1. Claims 18-21 depend directly from claim 17 and therefore contain each and every element of claim 17. Claim 26 depends directly from claim 24 and therefore contains each and every element of claim 24. Therefore, for the reasons already set forth for claims 1, 17, and 24, withdrawal of rejections of claims 2, 5-10, 15-16, 18-21, and 26-27 is respectfully requested.

Conclusion

Entry of this amendment is requested pursuant to MPEP 714.12 and 714.13 (37 CFR 1.116(b)) because the amendment remedies claim objections made by the examiner and thus removes issues for appeal, and places the application in better form for appeal.

Withdrawal of the rejections to this application is requested for the reasons set forth herein and a Notice of Allowance is earnestly solicited. If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 72255/00010.

Respectfully submitted,

Date: 6-25-09

Larry B. Donovan
Registration No. 47,230
TUCKER ELLIS & WEST LLP
1150 Huntington Bldg.
925 Euclid Ave.
Cleveland, Ohio 44115-1414
Customer No.: 23380
Tel.: (216) 696-3864
Fax: (216) 592-5009